**ORM for MeCo**

Liz Hinz

Professor Nathan Braun

CSD370-A339: Secure Software Development

May 18, 2025

**ORM for MeCo**

A solid understanding of Operational Risk Management (ORM) should be a priority at MeCo. Provided are three sources that cover ORM to help the company gain a thorough understanding of how it works, potential steps to take, and best practices on reducing risks.

Tom Sire on Pulsion's website describes having a risk management program as a way of mitigating risks and reducing costs (Sire, 2024). Having a risk management plan also helps boost productivity, better identify risks, and create a better experience for users and stakeholders (Sire, 2024). Developing a risk management plan means looking for business, operational, project, technical, and software risks (Sire, 2024). This involves project managers who help determine the risks and security vulnerabilities for developers and other stakeholders (Sire, 2024). Sire usually includes six steps within a risk management plan: "identify risks, analyze risks, prioritize risks, implement risk management techniques, monitor risks, and review risks" (Sire, 2024). Some best practices for reducing tasks include using management tools, identifying risks in projects, conducting a risk analysis, and constantly monitoring software for risks.

The Thomson Reuters website explains why operational risk is vital for an operation. Businesses are vulnerable when risk is not properly managed (Thomson Reuters, 2024). Risks can come from many sources, such as "human error, third parties, cybersecurity threats, external events, and government regulations" (Thomson Reuters, 2024). Operational risk management involves reducing unintentional risk in an organization (Thomson Reuters, 2024). According to Thomson Reuters (2024), the steps to the operational risk management process are determining operational risks, the likelihood of impact of those risks, how to mitigate risks, monitoring risks, and reporting findings. Some best practices on reducing risks include investing time to properly identify, assess, and mitigate risks (Thomson Reuters, 2024).

Another website that has information on operational risk management is Xygeni. Xygeni (2025) states that operational risk management is the "process of identifying, assessing, and minimizing risks caused by system failures, human error, or external threats". ORM helps a business run smoothly and continuously, reduces costs, and creates a better customer relationship (Xygeni, 2025). The provided steps are continuous monitoring, risk reporting, risk identification, risk assessment, and risk mitigation (Xygeni, 2025). Some of the best practices in reducing risks are fostering a risk awareness culture, implementing strong governance and oversight, leveraging automation, continuous education and training, shifting security left, prioritizing based on exploitability, securing infrastructure as code, and monitoring continuously (Xygeni, 2025).

After review, all three sources provide similar information. They all emphasize the importance of establishing an operational risk management program and focus on identifying, assessing, and mitigating all risks. All of the included sources would be suitable for MeCo. However, Pulsion's article best suits MeCo since the information and steps are the easiest to implement.

**References**

Sire, T. (2024, June 24). *Risk Management Software Development: Mitigate Critical Risks With Effective Management Strategies in Software Development - Pulsion Technology*. Pulsion Technology. https://www.pulsion.co.uk/blog/risk-management-software-development/

Thomson Reuters. (2024, February 20). *Operational risk management (ORM): An overview*. Thomson Reuters Law Blog. https://legal.thomsonreuters.com/blog/what-is-operational-risk-management/

Xygeni. (2025, March 24). *What Is Operational Risk Management? Best Practices*. Xygeni | Software Supply Chain Security. https://xygeni.io/blog/what-is-operational-risk-management-best-practices/